REMARKS

Claims 1-38 and 40-45 are pending in this application. Claims 1 and 10 have been amended to more clearly point out and distinctly claim that which Applicant regards as the invention. Claim 39 has been canceled. Claim 45 has been added. It is submitted that no new matter has been added.

Applicant wishes to note that all references to paragraphs of the application in the response are paragraphs of the substitute specification.

Claim Rejections – 35 U.S.C. § 112

The Examiner has rejected claims 1-44 under 35 U.S.C. §112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant respectfully traverses the rejection in view of the amendment to claims 1, 10 and 39.

As described in at least paragraphs [0002], [0004], [0013], [0038] and [0061] of the application, the present invention is directed to a computer implemented method of providing computer information to multiple users about the spread of computer or software viruses to computers in specified geographical areas over preceding time intervals and to provide an indication to the users of a trend about the spread of the computer or software viruses.

In response to the Examiner's rejection, claim 1 has been amended to delete "most active" and to recite a computer implemented method comprising the step of making available information about the of spread computer viruses at a given time in a series of selectable geographical areas. Claim 10 has been similarly amended to delete "most active" and to recite that the information includes a trend of spread of the detected computer virus. Claim 39 has been canceled.

Applicant submits that one skilled in the art that would clearly understand what is meant by the spread of computer viruses. Accordingly, Applicants respectfully requests reconsideration and withdrawal of the §112 rejection of claims 1-44.

Claim Rejections – 35 U.S.C. § 102(e)

The Examiner rejected claims 1-44 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0056116 (Bunker, V. et al.). Applicant respectfully traverses the rejection.

Background

The Bunker patent relates to a system and method for assessing the vulnerability of network systems to a cyber attack.

Vulnerability in the computer security field refers to a weakness in a system allowing an attacker (hacker) to penetrate a system in order to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system or the data and applications it hosts (See Bunker at paragraph [0005]. Vulnerabilities may result from several and different components such as weak passwords, software bugs or design codes in the system, a script code injection, a SQL injection etc. A computer virus or malware can use vulnerabilities for infecting the system, but a computer virus is not a cause of said condition and its presence on a computer is not an indication of vulnerability. In any case no mention about computer virus or malware appears in the Bunker patent addressing the issue of assessing vulnerability of computer network or systems.

Many software tools exist that can aid in the discovery (and sometimes removal) of vulnerabilities in a computer system. Though these tools can provide a good overview of possible vulnerabilities present, they impose a complete and thorough scan of the system to avoid false positives and a limited-scope view of the problems present in the system.

Bunker proposes, then, a scalable holistic system that is able to conduct tests for thousands of customers in any place in the world and which comprises, in a preferred embodiment, a Test Center and one or more Testers (paragraphs [0013] and [0014]).

Moreover in paragraph [0111] of Bunker it is explained that:

> *"The Testers house the arsenals of tools that can be used to conduct hundreds of thousands of hacker and security tests. The Tester can receive from the Gateway, via the Internet, basic test instructions that can be encrypted. The instructions inform the Tester which test to run, how to run it, what to collect from the customer system, etc. Every basic test can be an autonomous entity that can be responsible for only one piece of the entire test that can be conducted by multiple Testers in multiple waves from multiple locations. .....The information collected by each test about the customer systems is sent to the Gateway and from there to the Database to contribute to creation of a customer's system network configuration."*

Further, paragraph [0112] of Bunker provides a list of hacker tools that the preferred embodiment uses, none of which are tools for determining the presence of a virus within a computer.

In contrast to Bunker, the present invention does not attack a user's computer from an external computer with an attack simulation which mimics hackers (see paragraph [0086]) but only performs a virus checking if a user petitions to do a partial audit (see paragraph [0023] of the application) using a pre-installed virus checking program. The user, in exchange, obtains free access to information prepared by gathering results of explorations carried out in many computers and grouped by local areas.

Paragraph [0022] of the Bunker patent declares:

> *Only customers affected by the new security vulnerabilities can receive the alerts. The Early Warning Generator system filters the overload of information to provide accurate, relevant information to network administrators. Additionally, the known configuration of the customer can be updated every time a security vulnerability assessment can be performed, making it more likely that the alerts remain as accurate and relevant as possible.*

Paragraph [0021] of Bunker makes clear that Classification at the Vulnerability Library includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and or application(s).

By contrast in the present invention:

- no report about the client computer or network is captured nor distributed;

- information about the degree of spread of viruses in a local area is offered to any client having or not having a virus problem and pertaining to said local area or wishing to connect with. Further, information about the spread of a computer virus can be made accessible to any user (without the need for the user to scan or search the user's computer by simply connecting through a communication network to the central site.

There is no hint or suggestion in Bunker to provide the features of the present invention and therefore as a computer implemented method the present invention should be recognized as new and inventive.

Distinct Features Of The Invention

In order to accept that Bunker anticipates amended claim 1 in the present application, Bunker must disclose all the steps a) to f) of amended claim 1.

Step a)

The Examiner states that step a) is disclosed by Bunker in paragraph [0142].

Step a) recites "providing a computer virus utility program to a plurality of users distributed around different locations each of them operating at least one local computer."

In this case the Examiner appears to be equating a "Tester 502" (see also paragraphs [0014], [0017] and [0110]) to "computer virus utility program". In this regard, it should be taken into account that Bunker defines "Tester" among other paragraphs in the following paragraphs where the underlined part emphasizes the meaning of the definition:

> *[0018] The Testers can reside on the Internet, in a Web-hosted environment, and can be distributed geographically anyplace in the world. The entire test can be split up into tiny pieces, and it can also originate basic tests from multiple points and therefore be harder to detect and more realistic. The Testers house the arsenals of tools that can be used to conduct hundreds of thousands of hacker and security tests. The Tester can receive from the Gateway, via the Internet, basic test instructions that can be encrypted. The instructions inform the Tester which test to run, how to run it, what to collect from the customer system, etc. Every basic test can be an autonomous entity that can be responsible for only one piece of the entire test that can be conducted by multiple Testers in multiple waves from multiple locations. Each Tester can have many basic tests in operation simultaneously. The information collected by each test*

about the customer systems is sent to the Gateway and from there to the Database to contribute to creation of a customer's system network configuration.

In spite of the fact that in the summary of the invention it is said that "preferred embodiment provides real-time network security vulnerability assessment tests", no mention is made at all of using an antivirus or virus utility program. Moreover in the present invention, the virus utility program is distributed or offered to a plurality of users (and it has to be downloaded into the computer) while in Bunker "Testers" are located on the Internet or in a WEB hosted environment or Website [paragraphs [0018] and [0110]. No distribution of software tools is done in Bunker but these tools remain at the Tester center in order to perform there the vulnerability assessment operations.

Therefore step a) is not performed by Bunker.

Step b)

The Examiner states that step b) is disclosed by Bunker at paragraphs [0110 – 0111].

Step b) recites "obtaining information about geographical location of each of said local computers."

Paragraph [0110] describes the Testors as being distributed in different geographical locations on the Internet or in a WEB hosted environment or Website. As clearly stated, the Testors are described as being remote from the customer computers. Merely knowing the location of the Testors does not allow determining the location of the customer computers. Nor is their any suggestion in Bunker that a Test Center obtain information about the location of the customer computers.

Therefore step b) is not performed by Bunker.

Step c)

The Examiner states that step c) is disclosed by Bunker at paragraphs[184-185].

Step c) recites "carrying out, using said computer virus utility program, in response to a petition by said user, at least a computer virus search or scanning operation covering at least a part of at least one hard disk of said local computer or at least a part of a unit supporting information connected or connectable to said local computer."

In Bunker a full active host scan is performed across the entire range of network addresses supplied by the customers. However, the scan does not need to execute any special software in the user's computers under test. On the contrary according to the teachings of the present invention, a

"computer virus utility program" is downloaded and executed within each computer to be checked. This is a major difference between Bunker and the present invention.

Moreover in Bunker at paragraph [184], related to a "network survey", it is mentioned that a "full active host scan across the entire range of network addresses" is performed. This is in line with a vulnerability assessment that, as a person skilled in the field should recognize, imposes to completely examine the computer system and associated network. However, to implement the method according to the present invention and as stated in this step c), it is sufficient to look at "a part of a hard disc of said local computer, or a part of a unit supporting information connected or connectable to said local computer". Therefore, this way of operating is not at all feasible according to Bunker and no hint leads to the present invention and thus should be recognized as non-obvious and with inventive activity.

Looking closer to step c) and to the description in the specification of the present invention, it appears that the virus utility program is in fact offered (see paragraph [0023] mentioning that step c) is performed in general in response to a petition of the user) in exchange for receiving the information of step f) of the main claim. This distinguishing feature which removes any resemblance between the Bunker patent and the present invention is now added into amended claim 1 submitted for examination.

Therefore step c) is not performed by Bunker.

Step d)

Step d) recites "issuing a report containing the results of said computer virus search or scanning operation on said local computer including information about detected computer viruses and making available the results of said report through a communication network along with at least data of said geographical location of said local computer, to a center."

The Examiner states that Bunker discloses step d) at paragraphs [0195-212].

As clearly described by Bunker at paragraph [0197], any report issued by Bunker includes only information about the vulnerability to attack by a hacker and does not include any information about viruses detected on a computer. Another essential difference appears because, according to Bunker, reports about vulnerability are sent to the users or to a correspondent or named contact person monthly [0201], while in the present invention, reports are transmitted to a center where in a further step e) they are processed.

Therefore step d) is not performed by Bunker.

Step e)

Step e) recites "processing at said center a plurality of reports received from different local computers and allocating said detected computer viruses in geographical areas".

The Examiner states that Bunker discloses step e) at paragraphs [0195-212].

This step is not at all carried out in Bunker and cannot be assimilated to the tasks done in the quoted paragraphs. There is no allocation of detected computer viruses to geographical areas. As previously mentioned, Bunker only speaks about distributing the tools, i.e. "Testers" in different geographical areas.

Therefore step e) is not performed by Bunker.

Step f)

Step f) recites "making available information about the spread of at least one of said computer viruses at a given time in a series of selectable geographical areas corresponding to said different locations of step a)."

The Examiner states that step f) is disclosed by Bunker at paragraphs [0195-212].

Step f) is not implemented in Bunker. Bunker does not provide any information related to the spread of computer viruses detected related to a geographical area. In the very detailed vulnerability analysis of Bunker no mention is done of any classification of computer viruses by geographical areas, and no hint about this concept is disclosed.

In summary, as described above, Bunker describes a system for determining the vulnerability of computer systems to attack by a hacker. Bunker does not disclose, teach or suggest determining whether or not a computer virus is present in a computer as recited in amended claim 1. Further, Bunker does not teach or suggest making available information to users about the occurrence of viruses in computers in selectable geographic areas as recited in amended claim 1. For these and other reasons described above, Applicant respectfully requests reconsideration and withdrawal of the §102 rejection to claim 1.

Claims 2-38 and 40-45 are allowable as depending from allowable claim 1.

New claim 45 recites authorization of the user to send a report on the results of the virus checking. Support for claim 45 is found at paragraph [0045] of the application. New claim 45 is allowable at least by its dependency on claim 1.

Conclusion

Insofar as the Examiner's objections and rejections have been fully addressed, the instant application, including claims 1-38 and 40-45 is in condition for allowance and Notice of Allowability of claims 1-38 and 40-45 is therefore earnestly solicited.

Respectfully submitted,

MIKEL URIZARBARRENA AGUIRRE

February 21, 2008 By: _____
(Date)

LOUIS SICKLES II
Registration No. 45,803
PANITCH SCHWARZE BELISARIO & NADEL LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1330
Direct Dial: 215-965-1294
Facsimile: 215-965-1331
E-Mail: lsickles@panitchlaw.com

LS/msm